Ars Iuris Salmanticensis
TRIBUNA DE ACTUALIDAD
Vol. 4, 27-34
Diciembre 2016
eISSN: 2340-5155

La protección de datos que viene: el nuevo Reglamento General europeo

The forthcoming data protection: the new European General Regulation

Juan Pablo APARICIO VAQUERO[1]
Profesor Titular de Derecho Civil
Universidad de Salamanca

Fecha de recepción: 15 de octubre de 2016
Fecha de aceptación definitiva: 28 de octubre de 2016

Tras un par de años en los que parecía que había decaído el interés del legislador comunitario, a lo largo de 2015 se reactivó el proceso de elaboración de lo que, a la postre, fue publicado por el *Diario Oficial de la UE* el 4 de mayo de 2016 como *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, *de 27 de abril de 2016*, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)*. Dicha norma entró en vigor a los 20 días de su publicación, aunque su efectividad queda aplazada hasta el 25 de mayo de 2018; hasta entonces seguirá siendo de aplicación la normativa vigente.

1. Proyecto de Investigación «Privacidad y redes sociales: nuevos retos en la protección de datos y de los derechos al honor, intimidad e imagen» (Ref. DER2013-42294-R), financiado por el Ministerio de Economía y Competitividad *(Programa Estatal de Investigación*, *Desarrollo e Innovación Orientada a los Retos de la Sociedad)*.

Vemos a continuación algunas de sus principales *novedades*, con las que Europa trata de afrontar los retos de la privacidad en la Sociedad de la Información del siglo XXI.

Cabe destacar, en primer lugar, el instrumento normativo elegido: se trata de un *Reglamento* que sustituye a la anterior Directiva de 1995, lo cual es sumamente indicativo del interés europeo. Efectivamente, no se trata ya de aproximar o armonizar los ordenamientos estatales para que *todos* ellos tengan, a través de sus diferentes leyes, un contenido similar, siquiera sea con ciertos mínimos; por el contrario, se impone una *norma única*, con pretensiones de establecer un régimen completo (es extensa: 99 artículos, precedidos por hasta 173 Considerandos) para toda la Unión, y aplicable también a cualquiera que trate datos en el territorio de la misma. Así pues, en materia de protección de datos, Europa pasa a regirse por el axioma «un continente, una norma». El sistema de «ventanilla única» contribuye a reforzar dicha idea, permitiendo a los operadores dirigirse a una sola Autoridad nacional de protección de datos, aunque operen en varios países, quedando el Comité Europeo de Protección de Datos como garante de la aplicación de soluciones uniformes, resolviendo de forma vinculante cuando haya conflicto entre varias Autoridades implicadas.

El anterior principio tiene dos consecuencias inmediatas: por un lado, el Reglamento será de aplicación *también* a las empresas o responsables del tratamiento radicadas *fuera de la Unión* que ofrezcan servicios o bienes a interesados que residan en la Unión o controlen su comportamiento en territorio de la misma. Consagra así las interpretaciones de la Directiva europea (artículo 4) que venía haciendo el Grupo de Trabajo del artículo 29 (por ejemplo, en sus Dictámenes 1/2008, 5/2009, 8/2010 o 2/2013; también, en el Documento de Trabajo WP56, de 2002), en consonancia con el Considerando 20 de la misma, aunque bajo una perspectiva distinta: hasta el momento se hablaba de la ubicación de los medios o dispositivos, mientras que ahora se pone el foco *en las personas* en cuanto destinatarias de los servicios o cuyo comportamiento es objeto de control (la «orientación hacia las personas» de la que hablaba el citado Dictamen 8/2010). Evidentemente, dicho control se llevará a cabo a través de la recogida y tratamiento de datos a partir de sus dispositivos (teléfonos móviles, ordenadores, etc.), que son los que estarán en territorio de la Unión, pero el cambio de enfoque es significativo de la preocupación del legislador.

De otra parte, las legislaciones nacionales de los Estados miembros quedan automáticamente derogadas (*rectius*, «inaplicables») en todo lo regulado por el Reglamento. Ciertamente, éste contiene algunas remisiones a las normas internas, de manera que los Estados conservan aún ciertas posibilidades de actuación, aunque sean limitadas (así, por ejemplo, lo previsto en el artículo 8 en relación con la edad mínima para consentir lícitamente en el marco de la prestación de servicios de la Sociedad de la Información), pero fuera de ellas los Estados no podrán regular apenas sobre protección de datos, salvo las oportunas normas de desarrollo. Por lo que a España respecta, habrá que ver los problemas que ello plantea, dado que la regulación básica del *derecho*

Ars Iuris Salmanticensis,
vol. 4, diciembre 2016, 27-34
eISSN: 2340-5155

fundamental a la protección de datos (STC 292/2000, de 30 de noviembre de 2000) o «autodeterminación informativa» es objeto de reserva de Ley Orgánica. Además, hay otras cuestiones no expresamente recogidas en el Reglamento, como la obligación de inscripción en el Registro de la AEPD, sobre las que pueden suscitarse dudas: ¿seguirán vigentes? Por lo que a ésta en concreto respecta, a mi juicio no: una cosa es que los Estados puedan seguir legislando en lo no expresamente contemplado y otra que, dentro del marco del Reglamento y donde éste no haya querido establecer una concreta obligación (en este caso, a los responsables del tratamiento), los distintos países puedan imponerla, pues si así fuera se frustraría su carácter de «norma única» y continuaría la fragmentación nacional que ahora pretende superarse.

El Reglamento se asienta sobre dos grandes principios: el *consentimiento* y posibilidad efectiva de control por parte del titular de los datos, y la *proactividad* del responsable del tratamiento.

Por lo que respecta al *control* del titular de los datos, su *consentimiento* (cuando el tratamiento lo requiera) ha de ser *inequívoco*, *explícito* en ciertos casos (como el de los datos sensibles, entre los que ahora se contemplan expresamente los genéticos y biométricos) y *verificable*; por supuesto, y al igual que sucede hasta el momento, será siempre retirable, estableciéndose ahora que dicha *retirada* ha de ser tan fácil como dar el consentimiento. A diferencia de ciertas prácticas ahora toleradas, no cabe obtener el consentimiento del titular en base a su inacción o silencio, sino que exigirá una declaración expresa o acción positiva por su parte, tras haber recibido la oportuna información: adiós a las casillas premarcadas («si no desea que sus datos sean tratados, desmarque esta casilla») como práctica extendida que existe actualmente. La *verificabilidad*, por su parte, obliga a quienes recojan los datos a tratar a demostrar que el titular consintió efectivamente.

Evidentemente, el titular conserva los derechos que la normativa le reconocía hasta el momento: *acceso* a los datos, *rectificación*, *supresión* (el conocido hasta ahora en España como «cancelación») y *oposición*, así como no ser objeto de decisiones individuales basadas exclusivamente en procesos automatizados, incluida la elaboración de perfiles, salvo con su consentimiento expreso o por las otras causas justificadas que contempla el Reglamento. Todo ello, bajo los *principios de transparencia e información*, que implican que el titular debe recibir toda la información y comunicaciones relativas al tratamiento de sus datos, sobre todos los extremos relacionados y derechos reconocidos, de forma concisa, inteligible y fácilmente accesible. En cuanto al llamado «derecho al olvido» queda finalmente identificado (a mi juicio, acertadamente) con el derecho de supresión (así, en el propio título del artículo 17), obligándose a los responsables frente a los que se haya ejercitado a informar a cualesquiera otros de la necesidad de eliminar cualesquiera enlaces, copias o réplicas de los mismos. A la luz de la sentencia del *caso Google* (Sentencia del Tribunal de Justicia de 13 de mayo de 2014, asunto C 131/12), en su aplicación a la interpretación del nuevo art. 4.2, no hay

Ars Iuris Salmanticensis,
vol. 4, diciembre 2016, 27-34
eISSN: 2340-5155

duda de que buscadores y otros prestadores de servicios de la sociedad de la información realizan «tratamiento de datos» y son «responsables», por lo que frente a ellos cabe sin más el ejercicio del derecho de supresión, sin precisar del reconocimiento de ningún derecho *ad hoc*.

Sí se reconoce, sin embargo, un nuevo e interesantísimo derecho, el de «portabilidad de los datos» (artículo 20), que supone, cuantitativa y cualitativamente, un paso más allá del tradicional derecho de acceso: en ciertos casos, el titular puede solicitar al responsable la entrega de los datos que le facilitó y que lo haga en un formato estructurado, de uso común y lectura mecánica, para dárselos a otro responsable; puede solicitar, incluso, que tales datos se transmitan directamente entre ambos responsables (el antiguo y el nuevo), si es técnicamente posible. En el actual contexto de portabilidades telefónicas, redes sociales, servicios financieros *on line* y servicios de *cloud computing*, la utilidad de un derecho con tal alcance parece incuestionable, aunque pueden presentarse también importantes dificultades en su implementación práctica (por ejemplo, ¿*quid* de los datos generados durante el servicio que puedan ser propios del responsable?); además, el Reglamento tampoco aclara de cuánto tiempo dispone el primer responsable para dar respuesta a la petición del titular.

En cuanto a la *edad para prestar el consentimiento* nada dice el Reglamento, por lo que habrá que seguir atendiendo a las normativas nacionales sobre capacidad de obrar, en general, o sobre datos, en particular. Efectivamente, el artículo 8, que habla de las «condiciones aplicables al consentimiento del niño en relación con los servicios de la Sociedad de la Información» regula exclusivamente dicho supuesto, y no otro; y tampoco lo hace de forma única, pues el límite de 16 años para dar un consentimiento lícito es posible rebajarlo a 13 por los Estados miembros. Obsérvese que, frente al vigente artículo 13 del Reglamento de desarrollo de la LOPD, que se refiere a la capacidad del menor para prestar el consentimiento (cualquiera y en cualquier ámbito), el precepto europeo regula *sólo* el consentimiento *en el ámbito de un servicio de la Sociedad de la Información* (por ejemplo, inscribirse en una red social). En concurrencia de ambas normativas, por lo tanto, si se mantuviera la vigencia del artículo español (por otra parte, cuestionable y cuestionado, dado el rango de la norma, meramente reglamentaria, en que se regula tan importante cuestión, que afecta, sin duda, al núcleo del derecho fundamental), un menor en España podría prestar lícito consentimiento en el marco de servicios de la Sociedad de la Información a partir de los 14 años. En todo caso, la edad reconocida en ambas normativas no afecta en sí a la capacidad para prestar el consentimiento contractual (*vid*. la nueva redacción del art. 1263 CC), lo que, en función del tipo de negocio que se trate, puede dar lugar a la curiosa paradoja de que el menor pudiera disponer de sus datos (cuestión que afecta a sus derechos fundamentales y, además, puede ser necesaria para la celebración y ejecución del contrato), pero no prestar el propio consentimiento contractual (cuestión meramente patrimonial) lo que, *de facto*, le impediría facilitar aquéllos o resultaría un acto nulo o anulable.

Ars Iuris Salmanticensis,
vol. 4, diciembre 2016, 27-34
eISSN: 2340-5155

En cuanto a las empresas responsables del tratamiento, la clave es la «proactividad»: han de poder demostrar el cumplimiento de todos sus deberes u obligaciones *(accountability)*, y han de implementar todo tipo de medidas para garantizar el correcto ejercicio de sus obligaciones. Entre ellas destacan las llamadas privacidad por el diseño y por defecto (ambas contempladas en el artículo 25), así como la obligación de notificar las brechas de seguridad, la creación de la figura del Delegado de Protección de Datos y la realización de las llamadas «evaluaciones de impacto».

La privacidad por (o «desde») el diseño *(privacy by design)* supone la obligación del responsable del tratamiento de implementar la política de protección de datos en todos sus extremos desde el comienzo de cualquier proyecto, no como una última capa o revisión añadida una vez dicho proyecto está prácticamente listo, tal como ocurre muchas veces en la actualidad. En definitiva, la protección de datos debe ser un elemento más a considerar en cualquier nuevo plan de negocio o medida de desarrollo, en igualdad de condiciones que los demás factores técnicos, económicos o de oportunidad. En su virtud, ya desde el comienzo, se valorarán los datos a recabar de manera que sean los mínimos posibles, las medidas técnicas y organizativas de protección y la posibilidad de la llamada «seudonimización», que permite tratar datos de manera que sólo mediante el añadido de otros puedan atribuirse a un titular determinado; es decir, da una mayor libertad a la propia empresa, aun cuando el hecho de que todavía puedan llegar a permitir la identificación de un sujeto (la «anonimización» no es completa, de ahí el *palabro* que emplea la norma) obliga a adoptar medidas de protección.

De la misma manera, la privacidad por defecto *(privacy by default)* implica que al cliente o usuario se le ofrezca desde el principio el servicio con el mayor nivel de seguridad y privacidad, de manera que sea él mismo quien la rebaje mediante expresos actos de voluntad. En un rápido e intuitivo ejemplo, un prestador de servicios de red social deberá dar a una nueva cuenta el nivel más alto de privacidad, haciendo públicos por defecto los menores datos posibles, y sólo cuando el usuario expresamente lo permita a través de las opciones de configuración de dicha cuenta.

La *seguridad de los datos* ha de ser objetivo primordial de los responsables, de manera que deben incluso realizar las denominadas «evaluaciones de impacto en materia de protección de datos» (*EIPDs* o *PIAs*, por su acrónimo en inglés: *privacy impact assessments*). Dichas evaluaciones (artículo 35) suponen un obligado análisis del tratamiento a realizar cuando por su naturaleza, alcance, contexto o fines entrañe un alto riesgo para los derechos de los titulares, contemplando las operaciones a realizar, una evaluación de su necesidad, riesgos y medidas previstas para afrontarlos; la Autoridad de control elaborará y publicará una lista de los tipos de tratamiento que requieran la realización de PIAs. En España, la Agencia Española de Protección de Datos ya había publicado en 2014 una Guía sobre cómo llevar a cabo evaluaciones de este tipo, aun cuando no fuera (no lo sea, hasta el momento) obligatorio (http://www.agpd.es/

Ars Iuris Salmanticensis,
vol. 4, diciembre 2016, 27-34
eISSN: 2340-5155

portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf). Además, los responsables quedan ahora obligados a *notificar las roturas o violaciones de la seguridad* (*data breach notification*, artículos 33 y 34), en un plazo máximo de 72 horas, junto con las medidas adoptadas para ponerles remedio.

Por su parte, el *Delegado de Protección de Datos* (DPO, por sus siglas en inglés: *Data Protection Officer*) será el encargado de controlar internamente el cumplimiento de la normativa de protección de datos por parte del responsable y servir de enlace entre éste y la autoridad de control. La novedad de esta figura es relativa: lo es para España, cuya legislación actual no la recoge, pero no para otros Estados miembros, en los que ya existía con carácter obligatorio (así, Alemania) u opcional (por ejemplo, Austria u Holanda). En un término medio, el Reglamento no ha impuesto una obligación general de nombramiento de un DPO para todo responsable o encargado del tratamiento, pero sí para las administraciones públicas (salvo la judicial en el desempeño de su función) y para las entidades que monitoricen datos personales a gran escala, en particular si lo hacen sobre categorías especiales de datos (artículo 37).

Toda esta regulación se cierra con un *severo régimen de sanciones* a las infracciones tipificadas. Más allá de las indemnizaciones a los titulares perjudicados, las «multas administrativas» se impondrán teniendo en cuenta diversas circunstancias y podrán ascender a los diez millones de euros o hasta el 2% del volumen de negocio total anual global (nótese la importancia de cada uno de los adjetivos) de la empresa en el ejercicio financiero anterior, optándose por la de mayor cuantía entre ambas posibilidades. La voluntad disuasoria es clara, aunque, como todo, su efectividad dependerá de la interpretación de la norma y la valoración de las circunstancias concurrentes en cada caso.

Por lo demás, el Reglamento no viene solo. Es parte del llamado «paquete de protección de datos», que incluye a la *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo*, *de 27 de abril de 2016*, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención*, *investigación*, *detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales*, *y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo*. Esta Directiva extiende la regulación de la protección de datos a extremos no contemplados en la anterior Directiva de 1995 o el nuevo Reglamento, cuales son los relativos a los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

Y por lo que respecta a la transferencia internacional de datos, el nuevo *Privacy Shield* (Decisión de la Comisión C(2016) 4176 final, de 12 de julio de 2016) regula las transferencias con Estados Unidos en sustitución del anterior régimen del Puerto Seguro (*Safe Harbor*, aprobado por Decisión de la Comisión 2000/520/CE, de 26 de julio de 2000), que el Tribunal de Justicia, en su Sentencia de 6 de octubre de 2015 (asunto C-362/14, *caso Schrems*), declaró no conforme con el Derecho europeo. Bajo la prohibición de que la Comisión impidiera las competencias de las Autoridades Nacionales

para la valoración del nivel de protección que ofrecen los países destinatarios de los datos, el Tribunal sancionaba la nulidad del acuerdo alcanzado entre la misma y los Estados Unidos por no garantizar un nivel de protección suficiente («adecuada») para los ciudadanos europeos; efectivamente, era palmario que las empresas estadounidenses gozaban de grandes privilegios (así, por ejemplo, certificaban sus propios procedimientos de protección) y las autoridades estadounidenses tenían grandes poderes de acceso a los datos; frente a ello, el nuevo Acuerdo entre Europa y los EE. UU., que se desarrollará como «decisión de adecuación» prevista en el artículo 45 del Reglamento (equivalente al vigente artículo 25 de la Directiva, que lo ampara en la actualidad), permitirá la transferencia de datos sin necesidad de autorizaciones específicas, toda vez que el Gobierno estadounidense ha garantizado el no acceso generalizado a los datos y se imponen a sus empresas unas obligaciones de cumplimiento más riguroso, al tiempo que se prevén mecanismos para que los ciudadanos europeos puedan reclamar frente a posibles vulneraciones.

Aunque el Reglamento no sea eficaz hasta finales de mayo de 2018, obvia decir que conviene que las empresas vayan implementando las medidas oportunas para estar ya en condiciones de cumplirlo en tal fecha. Lo cierto es que el nuevo Reglamento no resulta contrario en prácticamente ningún extremo (quizá con salvedades como la mencionada sobre la inscripción de ficheros) a la normativa vigente, por lo que adelantar su cumplimiento no es sino una forma de responder a las obligaciones ya exigibles actualmente, así como una forma de ir detectando las prácticas deficientes o insuficientes que una empresa pudiera tener, para darles solución.

En definitiva, el nuevo Reglamento europeo pretende dar una respuesta global a la protección de datos, tanto desde la perspectiva del *titular* (reforzando su posición de *control* sobre los mismos y necesario consentimiento, aunque con la importante brecha que puede suponer autorizar el tratamiento lícito por parte del responsable siempre que éste tenga un «interés legítimo», *ex* art. 6.1.f en función de cómo se interprete dicho requisito) como desde la de las *empresas responsables y encargadas del tratamiento*, mediante la creación de un *marco seguro* para los nuevos desarrollos de la economía digital, basada en la *información como objeto de negocio*; y todo ello, en un ámbito territorial único (la Unión Europea), sin fragmentaciones.

Conviene insistir, por último, en la necesaria asunción de una *cultura de protección de datos*, por cuya virtud empresas y ciudadanos tomen conciencia de su importancia. Los datos personales son más que simples *accesorios* de la personalidad de los individuos: son su propia proyección en diversos ámbitos, definiendo su persona, afectándoles a nivel moral y económico (tienen un auténtico valor patrimonial). Se dice que los datos personales son el «petróleo del siglo XXI» y, en tal caso, conviene no olvidar que los yacimientos están (o *deben* estarlo) en poder de los sujetos particulares, bajo su control; hay muchos servicios que no son sino *plataformas de extracción de datos* de la «bolsa» que constituye la propia actividad de sus clientes. Efectivamente, servicios

Ars Iuris Salmanticensis,
vol. 4, diciembre 2016, 27-34
eISSN: 2340-5155

como las redes sociales, por ejemplo, aun cuando no exijan desembolso económico de sus usuarios, no son «gratuitos»: los datos personales suministrados son la moneda con la que aquéllos pagan al prestador y, siquiera sea por eso, los titulares han de hacer valer sus derechos. En estos contratos con auténtica *causa onerosa*, velar por la propia privacidad y control de los datos personales forma parte del viejo «ocuparse diligentemente de los asuntos propios» *(diligentiam quam in suis)*; lo mismo por la otra parte, que queda obligada a todas las consecuencias que deriven no sólo de la ley, sino también de la *buena fe*. Realmente, nada nuevo.

Ars Iuris Salmanticensis,
vol. 4, diciembre 2016, 27-34
eISSN: 2340-5155